Serial No. 10/559,889
Art Unit 4148

Docket No. PU030227
Customer No. 24498

Remarks/Arguments

The Office Action mailed October 1, 2008 has been reviewed and carefully considered.

An amendment to the specification has been made to correct a misspelling of the word "startup" as requested by the Examiner.

Claims 1-14 are now pending in this application. Reconsideration of the above-identified application, as herein amended and in view of the following remarks is respectfully requested.

Applicants have amended claims 1, 3-6 and 8 to unify terms and resolve antecedent basis objections raised by the Examiner.

Claims 1, 3-6, and 8 stand objected to by Examiner due to informalities relating to inconsistent use of terms.

Claims 6 and 14 stand rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 stands rejected under 35 USC §102(b) as being anticipated by US Patent No. 6,526,506 to Lewis (hereinafter "Lewis")

Claims 1, 7, and 13 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of US Patent No. 5,241,598 to Raith (hereinafter "Raith")

Claims 3, 4, and 14 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Raith and in further view of US Patent No. 7,293,289 to Loc et al. (hereinafter "Loc")

Claims 5 and 6 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Raith and in further view of US Patent No. 6,118,869 to Kelem et al. (hereinafter "Kelem").

Claim 9 stands rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Loc.

Claims 10, 11, and 12 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Kelem.

Claim Objections

Claims 1, 3-6, and 8 stand objected to by Examiner due to informalities relating to inconsistent use of terms. Applicant has amended these claims responsive to Examiner's objection and as such these claims are believed to be in condition for allowance.

35 U.S.C. §112 Rejection of Claims 6 and 14

Claims 6 and 14 stand rejected under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has amended these claims responsive to Examiner's rejection and as such these claims are believed to be in condition for allowance.

35 U.S.C. §102 Rejection of Claim 8

Claim 8 stands rejected under 35 USC §102(b) as being anticipated by Lewis. Applicants respectfully traverse the rejection.

Claim 8 recites, *inter alia*, "using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys." Thus, the present invention provides for a legacy encryption key retention mechanism in an access point. This allows for a more resilient key transition process while updating encryption keys (see, e.g., published application paragraphs 26 and 27).

In rejecting applicants' claims, the Examiner relies on Lewis which is directed to a multi-level encryption scheme for a wireless network (Lewis, abstract). Lewis teaches an encryption system in which mobile devices are manually configured by a system administrator with a "MASTER" encryption key, used to initiate access to the network (Col. 11, lines 1-10 and lines 17-20). A mobile device communicates with an access point using the "MASTER" key, and *the access point can not decrypt the packets because the master does not match the "ENCRYPT" key* used by the access point, and so then the access point relays the original message (without decrypting it) to a distribution key server residing on the hard-wired backbone network (Col. 11, lines 47-58). The key distribution server then responds with the "ENCRYPT" key so

the mobile device can begin communicating via the access point using the "ENCRYPT" key (Col. 11, lines 62-66).

The Examiner cites Col. 11, lines 49-54, 58-62 and Col. 12, lines 44-46 of Lewis as teaching, "and using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys." At Col. 11, lines 49-54 Lewis teaches:

> However, since the MASTER key will always be different from the ENCRYPT key such decryption will not be successful.
>
> Accordingly, the access point 54 is configured to forward the non-decrypted request packet in the manner described below in relation to FIG. 7.

Lewis teaches that during the initialization process, while the mobile sends packets using the MASTER key to the access point, that the access point can not decrypt it and consequently forwards the packet to the backbone (see, e.g., Lewis Col. 11, lines 45-49 and lines 54-58 for clarification of the context of the cited portion). At Col. 11, lines 58-62 Lewis states:

> The request packet is passed through the encryption engine 146 which the processor 142 provides with the MASTER key via line 148. As a result, the key distribution server 76 is able to successfully decrypt the request packet.

Lewis teaches how the key distribution server, a hardwired server residing on the backbone of the network, resolves and decrypts the initial request made by the mobile device using the MASTER key. (See Lewis Col. 11, lines 57-58 and lines 62-66 for clarification of the context of the cited portion). At Col. 12, lines 43-48, Lewis states:

> Periodically, the access point 54 may be instructed to use a different or new ENCRYPT key as discussed below. The access point 54, in this case, however, can communicate the new ENCRYPT key using the previous ENCRYPT key so as to maintain a secure wireless link even when updating the mobile terminal 66.

Lewis teaches that when an access point is instructed by a key distribution server) to change an "ENCRYPT" key, that the access point delivers the new ENCRYPT key using the old ENCRYPT key (See Lewis., Col. 14, lines 8-15 which discuss how key distribution server controls and updates access points.)

Nowhere in the cited portions of Lewis or the remainder of the patent is an access point disclosed which retains an old encryption key and a current encryption

key, and where the old encryption key is retained for use in the event of an encryption key update failure. As such, Lewis does not remotely teach or suggest, "using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys," as recited in Claim 8.

Accordingly, Claim 8 is believed to be in condition for allowance for at least the reasons stated above. Dependent Claims 9-12 include further distinctions over the cited reference and are also believed to be in condition for allowance at least due to their dependency from Claim 8. Early and favorable reconsideration of the rejection is earnestly solicited.

35 U.S.C. §103 Rejection of Claims 1, 7, and 13

Claims 1, 7, and 13 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Raith.

Claim 1 recites, *inter alia*, "wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key," which, similar to the above recited portion of Claim 8, represents the present inventions ability to provide for a legacy encryption key retention mechanism in an access point to ensure encryption does not fail during a key change procedure (see, e.g., published application paragraphs 26 and 27).

As was the case with Claim 8, the Examiner cites Col. 11, lines 49-54, 58-62 and Col. 12 lines 44-46 of Lewis as teaching "wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key."

In these cited portions, Lewis teaches: 1) that during the initialization process, while the mobile sends packets using the MASTER key to the access point, that the access point can not decrypt it and consequently forwards the packet to the backbone; 2) how the key distribution server, a hardwired server residing on the backbone of the network, resolves and decrypts the initial request made by the mobile device using the MASTER key; and 3) when an access point is instructed by a key distribution server to change an "ENCRYPT" key, that the access point delivers the new ENCRYPT key using the old ENCRYPT key. As such, Lewis does not remotely teach or suggest, "wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key," as recited in Claim 1.

Further, Claim 1 recites, *inter alia*, "resetting the old encryption key to equal an encryption key being used by a station in communication with the access point." Thus, the present invention is allowing an access point to retain an encryption key being used by a station as an "old encryption key" for backup purposes in the event of an encryption key transition failure.

With respect to this limitation of Claim 1, Examiner cites Col. 1, lines 32-35, Col. 34, lines 44-45, and lines 64-65 of Raith. At Col. 1, lines 32-35 Raith teaches:

> a method and apparatus for resynchronizing a rolling key used in the validation and verification of base stations and mobile stations within a cellular radio communications system.

Raith teaches the goal of resynchronizing cellular mobile stations with base stations. At Col. 34, lines 43-45 Raith teaches (emphasis added):

> At the beginning of each call, the *mobile station replaces* the value of the S-key$_{s\text{-}p}$ with the value of the S-key-next$_{s\text{-}p}$.

Hence, Raith teaches that a cellular phone will cycle in a new key to be used with each new call. At Col. 34, lines 63-66 Raith teaches (emphasis added):

> At blocks 400, 410, the *mobile station sets* the values of B'-key$_s$ and S'-key$_s$ equal to the values of B-key$_{s\text{-}p}$ and S-key$_{s\text{-}p}$, respectively.

Hence, Raith teaches that a cellular phone will store its current keys upon receiving a synchronization reset notification from the network (typically caused when an HLR fails). (See Raith Col. 34, lines 61-63 which describes that the key storage by a mobile device *only* occurs upon a B-key reset. See also Col. 32, lines 3-8 which discusses the network initiated reset and Col. 36, lines 40-44 which discusses the cause of a B-key reset). Raith does not teach an access point retaining an encryption key being used by a station as an "old encryption key" for backup purposes in the event of an encryption key transition failure. As such, Raith does not remotely teach or suggest at least, "resetting the old encryption key to equal an encryption key being used by a station in communication with the access point."

Accordingly, Claim 1 is believed to be patentable over the cited references taken singly or in any combination for at least the reasons stated above. Dependent Claims 3-7 and 13-14 include further distinctions over the cited reference and are also believed to be in condition for allowance at least due to their dependency from Claim 1. Early and favorable reconsideration of the rejection is earnestly solicited.

35 U.S.C. §103 Rejection of Claims 3, 4, and 14

Claims 3, 4, and 14 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Raith and in further view of Loc. Claims 3, 4, and 14 depend from Claim 1. The Loc patent does not cure the deficiencies of the Lewis and Raith patents. Therefore, claims 3, 4 and 14 are patentable for at least the reasons cited above with respect to the patents to Lewis and Raith.

35 U.S.C. §103 Rejection of Claims 5 and 6

Claims 5 and 6 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Raith and in further view of Kelem. Claims 5 and 6 depend from Claim 1. The Kelem patent does not cure the deficiencies of the Lewis and Raith patents. Therefore, claims 5 and 6 are patentable for at least the reasons cited above with respect to the patents to Lewis and Raith.

35 U.S.C. §103 Rejection of Claims 9

Claim 9 stands rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Loc. Claim 9 depends from Claim 8. As such, Claim 9 is patentable for at least the reasons cited above with respect to the patent to Lewis.

35 U.S.C. §103 Rejection of Claims 10, 11, and 12

Claims 10, 11, and 12 stand rejected under 35 USC §103(a) as being unpatentable over Lewis in view of Kelem. Claims 10-12 depend from Claim 8. As such, Claims 10-12 are patentable for at least the reasons cited above with respect to the patent to Lewis.

Conclusion

In view of the foregoing amendments to the claims and the accompany remarks, applicants solicits entry of this amendment and allowance of the claims. If the Examiner cannot take such action, the Examiner should contact the applicant's attorney at (609) 734-6820 for a telephonic interview.

No fees are believed due with regard to this Amendment. Please charge and fee or credit any overpayment to Deposit Account No. 07-0832.

Respectfully submitted,
Junbiao Zhang, et al.

By: _____
Robert B. Levy, Attorney
Reg. No. 28,234
Phone (609) 734-6820

Patent Operations
Thomson Licensing LLC
P.O. Box 5312
Princeton, New Jersey 08543-5312
18 December 2008